UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 4:19-cr-00980-HEA-JMB
	)	
HAITAO XIANG,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE IN OPPOSITION
TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

COMES NOW the United States of America, by and through its attorneys, Sayler A. Fleming, United States Attorney for the Eastern District of Missouri, and undersigned counsel, and for its Response in Opposition to the Defendant's Motion to Suppress Evidence, states as follows.

I. Background

On June 10, 2017, the defendant was preparing to board an international flight. He had a one-way ticket to China and had left his job at Monsanto just two days prior. Monsanto had previously alerted the FBI that the defendant had shared technical information with a competitor, emailed confidential information to himself, and conducted suspicious Google searches regarding sharing proprietary information with third parties. Monsanto also told the FBI that the defendant had provided deceptive answers during his exit interview, including when asked about the taking of proprietary information from Monsanto.

The FBI coordinated with the Department of Homeland Security Customs and Border Protection ("CBP"), who is responsible for enforcing federal law at the border and authorized to prevent transnational crime. CBP officers placed a lookout on the defendant. As he prepared to

board his flight, they stopped the defendant, searched his luggage, detained his electronic devices, and provided the devices to the FBI for assistance in analyzing the contents. The FBI reviewed three of the devices and located information that appeared to be proprietary to Monsanto. The FBI promptly conferred with Monsanto, who confirmed that the defendant possessed valuable trade secret information. No circuit court has required a warrant under these circumstances. The government expects to elicit the following facts at a hearing on the motion.

A. The Defendant's Departure from Monsanto

The defendant, a citizen of the People's Republic of China ("PRC"), worked for Monsanto and its subsidiary The Climate Corporation ("TCC") from 2008 until June 9, 2017. TCC uses complex analytics to improve farmers' profitability. Monsanto acquired TCC in October 2013. In 2014, the defendant moved from Monsanto to TCC, where he worked as an Advanced Imaging Scientist in their Technology Unit-Crop Analytics Subdivision. For purposes of this response, the government will refer to Monsanto and TCC as "Monsanto."

1. Monsanto Informs the FBI About the Defendant's Suspicious Activity

On May 24, 2017, the defendant verbally notified Monsanto of his intent to resign from the company. The next day, the defendant submitted his letter of resignation. On June 5, 2017, employees of Monsanto's security department informed FBI Special Agent Jaret Depke of several suspicious facts about the defendant.

First, they told SA Depke that the defendant had significant contact, including emails, with a former coworker ("Person 1"). The FBI had previously investigation Person 1 for stealing trade secrets from Monsanto. Person 1 worked for Monsanto from 2010 to 2014 and for TCC from 2014 to June 1, 2016. Although the investigation did not result in any charges, the FBI learned that after resigning from Monsanto, Person 1 accessed a cloud storage device and copied sixty-three files

containing trade secret information that belonged to Monsanto. The FBI also determined that Person 1 emailed some of Monsanto's trade secret information to his personal email account and his wife's personal email account in 2014 and 2015. Shortly before resigning from Monsanto, Person 1 traveled to the PRC with his corporate laptop for a job interview with Sinochem China National Seed Company, a competitor of Monsanto. Person 1 took the laptop, which was capable of accessing Monsanto's cloud storage accounts, to his job interview. Sinochem offered Person 1 a job on the spot. He accepted and has not returned to the United States.

Second, the Monsanto employees said they had conducted an internal review of the defendant's activity on their computer systems. They told SA Depke the defendant had conducted a number of suspicious Google searches, including queries along the lines of, "what happens if I give company information to a third party." The Monsanto employees also related that the defendant sent "packets of information" to NERCITA, a Chinese equivalent of TCC. At the point they communicated this to the FBI, the Monsanto employees did not know exactly what type of the information the defendant sent to NERCITA, whether the "packets" contained Monsanto's intellectual property, or whether the defendant had a legitimate reason for sending this information. The Monsanto employees explained that their internal review also revealed that the defendant sent multiple emails from his Monsanto email account to his personal email account. These emails contained information that was confidential, according to the Monsanto employees.

Monsanto scheduled the defendant's exit interview for June 9, 2017, which was also his last day of employment at the company. The day before the interview, Monsanto employees met with SA Depke to discuss their interview plan and provide additional information about the defendant. One of the Monsanto employees related that the defendant said he was leaving Monsanto to start a joint venture with a University of Illinois professor. The Monsanto employees

provided an internet address for the joint venture, AgSensus. According to the website, AgSensus was a start-up company purportedly funded in part by the National Science Foundation. The FBI determined that AgSensus was going to be an agricultural business and to some extent possibly a competitor of Monsanto.

2. The Defendant's Exit Interview

The next day, the defendant had his exit interview at Monsanto. During the interview, the defendant stated that he was leaving Monsanto to pursue a joint venture with a University of Illinois professor. The defendant signed and acknowledged his Employment Agreement and Proprietary Information and Inventions Agreement Reminder and Termination Certification. In these documents, the defendant certified, among other things, that: "(he) did not have in (his) possession, nor failed to return, any devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, materials, equipment, any other documents or property, or reproductions of any and all aforementioned items belonging to TCC, its subsidiaries, affiliates, successors or assigns." He further agreed that

> in compliance with the At-Will Employment, Confidential Information, Invention Assignment, and Arbitration Agreement, (he) will preserve as confidential all (TCC) Confidential Information and Associated Third Party Confidential Information, including trade secrets, confidential knowledge, data, or other proprietary information relating to products, processes, know-how, designs, formulas, developmental or experimental work, computer programs, databases, other original works of authorship, customer lists, business plans, financial information, or other subject matter pertaining to any business of (TCC) or any of its employees, clients, consultants, or licensees.

On his Termination Certification, the defendant listed his new position as co-founder and chief scientist of the joint venture.

On June 9, 2017, Monsanto employees met with SA Depke to describe the defendant's exit interview and provide additional information about their internal review. The employees

characterized the defendant's demeanor during the interview as "blatantly deceptive." They said he appeared nervous and deceptive when asked about returning all of Monsanto's property, when asked whether he retained any such property, and when confronted with the Google searches he had conducted. The Monsanto employees added that that these searches occurred in 2015 and 2016. The defendant claimed that he had a tumultuous relationship with Person 1, the Monsanto employee whom the FBI had previously investigated. The defendant also claimed that the defendant co-owned the joint venture. The same day, Monsanto employees provided the FBI with copies of the defendant's suspicious Google searches. The queries included search terms such as "company information to a third party; . . . . as evidence to accuse me; . . . . I will be cautious;" and "to be a piece of evidence that."

B. CBP Officers Search the Defendant's Luggage at the Border

After receiving this information, SA Depke contacted Art Beck, a Department of Homeland Security Customs and Border Protection ("CBP") Task Force Officer ("TFO") on the FBI's St. Louis Joint Terrorism Task Force. SA Depke asked TFO Beck to notify him if the defendant scheduled any outbound international travel and inquired as to whether CBP could conduct an outbound border search of the defendant. SA Depke provided TFO Beck with background on the defendant and described the circumstances surrounding his resignation from Monsanto. SA Depke and TFO Beck discussed whether CBP should exercise its authority to conduct searches of persons and merchandise crossing our nation's border. At this time, SA Depke and TFO Beck did not know if the defendant was planning to travel internationally.

It is common for federal agencies to collaborate, share information, and coordinate. In this case, CBP is the law enforcement agency charged with securing the borders. If the FBI is concerned that an individual is engaged in transnational criminal activity, such as transnational

theft of intellectual property or economic espionage, the FBI would logically alert CBP so that CBP can interdict the stolen property and investigate ongoing criminal activity.

TFO Beck placed a "lookout" on the defendant. TFO Beck told SA Depke that the lookout included a direction to interview and inspect the defendant and his property at the border. TFO Beck and SA Depke discussed their expectation that the defendant's electronic devices would likely contain a great deal of technical information and material in Mandarin. They concluded that CBP would likely need assistance from the FBI to inspect the devices since the FBI's St. Louis Field Office had ready access to Monsanto, whose headquarters were in St. Louis, and a Mandarin interpreter.[1] CBP policy governing border searches of electronic devices recognizes that there are situations where CBP officers may require assistance—either subject matter or technical assistance—to complete a border search of electronic devices. CBP Directive No. 3340-049A, *Border Searches of Electronic* Devices, § 5.4.2 (Jan. 4, 2018). SA Depke said that he wished to confer with his Chief Division Counsel and the U.S. Attorney's Office to ensure that the FBI had authority to review and analyze any electronics recovered from the defendant.

On June 8, 2017, TFO Beck informed SA Depke that the defendant had booked a one-way plane ticket from Chicago, Illinois to Shanghai, China. The reservation was for Saturday, June 10, 2017, the day after the defendant's departure from Monsanto. This was the first time that SA Depke learned the defendant planned to leave the country.

On June 10, 2017, the defendant obtained a one-way car rental and drove to O'Hare International Airport in Chicago, Illinois. The defendant was scheduled to fly from Chicago to Toronto and then on to Shanghai. As the defendant prepared to board his flight to Toronto, CBP

[1] As it turned out, when they later executed a search warrant on the defendant's electronic devices, the FBI located numerous relevant electronic documents in Mandarin.

agents met him on the jetway. They conducted an outbound border search of his checked and carry-on luggage. During this inspection, officers detained the following electronic devices: (1) a Lenovo Ideapad 1105-111BR laptop computer serial number YD0215RM, (2) a Samsung Galaxy S5 cellular telephone, (3) a thumbdrive labelled "Bio Net Solutions Inc," (4) an AT&T SIM Card, (5) an H20 wireless 4G LTE Smart SIM Card ACT FAST Code 153680486, and (6) a Toshiba 32 Gigabyte Micro SD Card[2] (collectively, "the Devices"). Additionally, during the border search, the defendant told CBP officers that he was traveling to the PRC for one month to visit his parents and vacation. The defendant told CBP officers he would officially join the previously-described joint venture in one week. SA Depke and TFO Beck knew the defendant had not purchased a return flight to the United States.

C. The FBI Takes Custody of the Devices and Reviews Them

CBP officers detained the Devices and gave them to a FBI Special Agent in Chicago. They instructed her to send the Devices to the FBI's St. Louis Field Office, Attention TFO Beck or SA Depke. The Devices arrived in St. Louis on June 13, 2017. At that time, TFO Beck was out of town, and SA Depke took custody of the Devices. On June 14, 2017, after conferring with Assistant United States Attorneys in St. Louis, SA Depke provided the Devices to the FBI St. Louis's Computer Analysis and Response Team ("CART").

The CART team began to create forensic images of three electronic devices: the Micro SD card, the thumb drive, and one of the SIM cards. A Micro SD card is a type of removable memory card that can be used in a variety of electronics. A thumb or USB drive is another type of removable memory that is typically used with a computer. A SIM card is a type of memory card

[2] CBP did not list the Micro SD card on its inventory. The FBI subsequently located the card, which had been inserted into the Lenovo laptop.

used in cellular telephones. A SIM card typically contains the subscriber information that enables the phone to use a cellular network.

Approximately six days passed while the FBI created the forensic images; made the data available to SA Depke; and trained him on CAIR, the FBI's review platform. On June 20, 2017, SA Depke conducted a quick keyword search of the forensic images using terms like "intellectual property" and "trade secret." The thumb drive was blank and had no data. On the Micro SD card, SA Depke located six electronic files that he suspected contained Monsanto's proprietary information.

On June 21, 2017, SA Depke provided Monsanto employees familiar with the investigation with copies of these files. SA Depke had to hand-deliver the files because they were subject to handling restrictions imposed by Monsanto. On June 28, 2017, Monsanto's Director of Business Conduct informed SA Depke that all six files contained proprietary information and that at least three of the files contained information he described as highly sensitive, proprietary, and confidential. The Director of Business Conduct informed SA Depke that Monsanto considered the data and information in these three files to be Monsanto's intellectual property and trade secrets. Monsanto employees also informed SA Depke that the defendant was not permitted to possess any of the aforementioned material after he left Monsanto.

On July 26, 2017, SA Depke obtained a search warrant (Cause No. 4:17MJ1245JMB) authorizing the seizure and examination of the Devices and the extraction from that property of electronically stored information. CART then created new forensic images of the devices. On August 2, 2017, SA Depke executed the search warrant and located multiple pieces of evidence on the Devices. In particular, the FBI found documents containing Monsanto intellectual property (including documents that were officially marked by Monsanto as "trade secrets"); email and chat

accounts used by the defendant that were previously unknown to the FBI; and travel records, emails and text messages, including communications surrounding the recruitment of the defendant into the Hundred Talents Program ("HTP"), the work he has conducted as a member of the HTP, and numerous documents providing insight into the HTP as a whole.

According to the FBI, the PRC oversees the HTP and hundreds of other Talent Plans. The Talent Plans are programs established by the PRC government to recruit individuals with access to or knowledge of foreign technology or intellectual property. Through these plans and other means, the PRC government has created a significant financial incentive for talented individuals residing outside of mainland China to transfer international technology and intellectual property to China, licitly or otherwise.

II. Argument

The defendant contends that because of the sensitive personal information typically contained on cellular telephones and digital media, searches of these items do not fall within the longstanding border search exception. He also contends that suppression is warranted because the FBI attempted to circumvent the warrant requirement by coordinating with CBP and by reviewing the defendant's electronic devices.

The defendant's motion should be denied. Border searches of electronic devices and media do not require a warrant or probable cause. And, assuming arguendo, that the border search in question required reasonable suspicion—the highest standard that has been applied to any border search—reasonable suspicion was clearly present here. Finally, there was nothing about the conduct of the specific search in this case that violated the Fourth Amendment.

A. Border Searches Do Not Require Warrants or Probable Cause

Searches and seizures of persons and their effects at the border constitute a long-recognized exception to the Fourth Amendment's warrant requirement. *United States v. Ramsey*, 431 U.S. 606, 616–19 (1977). The authority to conduct warrantless border searches and seizures advances the United States' "inherent authority" and "paramount interest" in protecting its "territorial integrity," which "is at its zenith" at the border. *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004); *see also United States v. Ickes*, 393 F.3d 501, 506 (4th Cir. 2005) (characterizing the government's interest as "overriding"). This substantially elevated governmental interest renders "the Fourth Amendment's balance of reasonableness . . . qualitatively different at the international border than in the interior," specifically, "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is . . . struck much more favorably to the Government." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538–40 (1985) (internal citation omitted); *see also Ramsey*, 431 U.S. at 623 n.17 (recognizing lack of "statutorily created expectation of privacy" at the border and the "constitutionally authorized right of customs officials" to search persons and goods at the border).

The border search and seizure authority granted to customs officers is broad and is codified in numerous statutes and regulations. Congress has defined customs officers to include "any officer of the United States Customs Service of the Treasury Department . . . or . . . of the Coast Guard, or any agent or other person, including foreign law enforcement officers, authorized by law or designated by the Secretary of the Treasury to perform any duties of an officer of the Customs

Service." 19 U.S.C. § 1401(i).[3]

Accordingly, customs officers working for CBP have border search authority. Although only certain officials are empowered to initiate border searches, the participation of other government personnel in the search is permissible. *See, e.g.*, *United States v. Boumelhem*, 339 F.3d 414, 423 (6th Cir. 2003) (rejecting argument that a border search was "tainted by participation or direction of the FBI"); *United States v. Alfonso*, 759 F.2d 728, 735 & n.2 (9th Cir. 1985) (remarking that the participation of an FBI agent in a border search conducted by a customs officer would not taint the border search); *United States v. Schoor*, 597 F.2d 1303, 1306 (9th Cir. 1979) (upholding a border search where DEA agents, who lacked probable cause, advised customs officials of certain information and asked customs officers to search two passengers entering the country). In fact, Congress has recognized that customs officers may enlist the assistance of others—whether government officials or civilians—to conduct a border search. The source of this authority is 19 U.S.C. § 507, which provides that every customs officer has "the authority to *demand the assistance of any person* in making any arrest, search, or seizure authorized by any law enforced or administered by customs officers if such assistance may be necessary" (emphasis added).

Customs officers' border authority includes the right to: inspect and search any vehicle or vessel and all persons, packages and cargo therein, *see* 19 U.S.C. §§ 482, 1467, 1581; inspect and search all persons, baggage, and merchandise entering the United States, *see* 19 U.S.C. §§ 1496, 1582, and 19 C.F.R. § 162.6; detain and search all persons entering from foreign countries, *see* 19 U.S.C. § 1582; and detain property until inspected, examined, found to comply with the law, and

[3] The Homeland Security Act of 2002 transferred the functions and personnel of the United States Customs Service from the Department of the Treasury to the Department of Homeland Security. 6 U.S.C. § 203(1). These functions were subsequently delegated to CBP.

cleared for release, *see* 19 U.S.C. §§ 1461, 1499. Similar broad authority "to conduct routine searches and seizures at the border, without probable cause or a warrant" has existed "[s]ince the founding of our Republic." *Montoya de Hernandez*, 473 U.S. at 537 (citing *Ramsey*, 431 U.S. at 616–17).

Only once has the Supreme Court ever required any heightened suspicion to justify a border search or seizure, and that case involved the extreme factual situation of a prolonged detention of a defendant—suspected of smuggling drugs in her alimentary canal—for a monitored bowel movement. *Montoya de Hernandez*, 473 U.S. at 534–36, 541–42. The Court specifically refrained from defining further "what level of suspicion, if any, [would be] required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches," *id.* at 541 n.4, and, in cases involving border searches of property, the Court has rejected lower court decisions cabining the government's plenary border search authority. *See, e.g.*, *Flores-Montano*, 541 U.S. at 150 (overturning Ninth Circuit decision requiring reasonable suspicion to conduct a border search of an automobile gas tank); *Ramsey*, 431 U.S. at 607–08, 620–24 (overturning D.C. Circuit decision requiring probable cause and a warrant before opening international mail). *Montoya de Hernandez* and *Flores-Montana* each reflect the Supreme Court's hesitance to unduly constrain the sovereign's border authority by arbitrarily assigning higher levels of privacy at the border to particular categories or items, or to particular types of searches.

B. The Border Search of the Defendant's Devices Was Lawful

Here, the inspection of the defendant's electronic devices does not fall within any category that the Supreme Court has recognized requires reasonable suspicion. As an initial matter, the search was of his *property* not his person, let alone the highly intrusive searches the Court has found to require reasonable suspicion. *See Flores-Montano*, 541 U.S. at 152. The Supreme Court

has been "unwilling to distinguish between different kinds of property" at the border, and this search should be treated as any other property search that only requires reasonable suspicion if it is unreasonably offensive or destructive. *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018). The Supreme Court's border search cases jurisprudence makes clear that the government's authority at the border allows for suspicionless searches of property that are not unreasonably intrusive, offensive, or destructive. *Flores-Montano*, 541 U.S. at 152; *Montoya de Hernandez*, 473 U.S. at 538. Under this well-established authority, these searches should therefore be considered routine.

Even if individualized suspicion was required, CBP was notified in advance of the FBI's reasonable suspicion of the defendant. Specifically, SA Depke provided CBP with background on the defendant and described the circumstances surrounding his resignation from Monsanto. SA Depke and TFO Beck discussed the possibility of CBP exercising its authority to conduct a border inspection should the defendant travel internationally. Once the defendant presented himself for inspection at the international border, CBP officers conducted a border inspection of the defendant and his personal effects, and detained certain electronic devices found during that inspection. Because SA Depke and TFO Beck expected to recover a great deal of technical data as well information in Mandarin (as noted, the defendant is a PRC citizen), they determined that CBP would need the FBI's assistance to complete the border search. *See* CBP Directive No. 3340-049A, *Border Searches of Electronic Devices* (Jan. 4, 2018) § 5.4.2 (setting forth CBP's policy parameters for seeking technical and subject matter assistance).[4]

In Chicago, CBP officers provided the Devices to the FBI for review in St. Louis to provide

[4] CBP's policy directive governing border searches of electronic devices recognizes that CBP Officers "may sometimes need technical assistance to render a device and its contents in a condition that allows for inspection." § 5.4.2.1. Such technical assistance may include issues

the requested assistance. SA Depke took custody of the devices when TFO Beck was out of town. SA Depke conducted a cursory review of three of the memory cards; located technical, proprietary information on them; promptly contacted Monsanto to better understand the information; and obtained a search warrant to conduct a more comprehensive review of the Devices. In sum, CBP and the FBI acted reasonably and consistent with the border search exception.

1. Warrants and Probable Cause Are Not Required for Border Searches of Electronic Devices

When reviewing border searches of electronic devices, some courts have distinguished between basic or manual searches and advanced or forensic searches.[5] A manual search is limited to the information viewable on the device through its native operating system. By contrast, a forensic search typically involves comprehensive copying and analysis of all the data (including deleted data) resident on an electronic device. *See United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (explaining that a forensic search is "a powerful tool capable of unlocking password-protected files, restoring deleted material, and retrieving images viewed on web sites," *id.* at 957, with the ability to access "deleted files" that "cannot be seen or accessed by the user without the

---

relating to password protection or encryption, as well as translations assistance. *Id.* The policy also addresses the circumstances where CBP may seek subject matter assistance, which entails "referral to subject matter experts to determine the meaning, context, or value of information contained" on the device. *Id.* § 5.4.2.2.

[5] CBP's Directive distinguishes between "basic" and "advanced" searches and follows different procedures for each. CBP Directive No. 3340-049A §§ 5.1.3, 5.1.4. An "advanced search" is "any search in which an Officer connects external equipment, through a wired or wireless connection, to an electronic device not merely to gain access to the device, but to review, copy, and/or analyze its contents." *Id.* § 5.1.4. A "basic search" is "[a]ny border search of an electronic device that is not an advanced search." *Id.* § 5.1.3. For all practical purposes, any search of a device that those courts have described as "forensic" would constitute an "advanced" search under the CBP Directive, and therefore would be subject to a reasonable-suspicion requirement under the Directive. However, not all advanced searches would necessarily qualify as "forensic" searches, but that distinction is immaterial to the resolution of the instant motion.

use of forensic software," *id.* at 958 n.5, resulting in a search that is "comprehensive and intrusive [in] nature," which "cop[ies] the hard drive and then analyze[s] it in its entirety, including data that ostensibly has been deleted," *id*. at 962).

Every circuit court to have considered this issue has held that no degree of suspicion is required for manual searches. *See, e.g.*, *Alasaad v. Mayorkas*, Nos. 20-1077, 201081, -- F.3d --, 2021 WL 521570 at *7 (1st Cir. Feb. 9, 2021) ("We . . . agree with the holdings of the Ninth and Eleventh circuits that basic border searches . . . need not be supported by reasonable suspicion); *United States v. Kolsuz*, 890 F.3d 133, 147 n.5 (4th Cir. 2018) (stating that *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005) "treated a [basic] search of a computer as a routine border search, requiring no individualized suspicion for the search'"); *United States v. Arnold*, 533 F.3d 1003, 1009-10 (9th Cir. 2008) (holding that reasonable suspicion was not required for manual search of laptop computer at the border); *United States v. Linarez-Delgado*, 259 F. App'x 506, 508 (3d Cir. 2007) (citing *Ickes* and holding that viewing of camcorder footage was a lawful border search that did not require a warrant or reasonable suspicion); *see also Cotterman*, 709 F.3d at 960-67 (observing that manual border searches of electronic devices require no individualized suspicion as held in *Arnold*).

Several circuits have found, or assumed without holding, that reasonable suspicion is necessary for forensic searches, although the Eleventh Circuit has held that no degree of suspicion is required. *Compare United States v. Aigbekaen*, 943 F.3d 713, 719 n.4 (4th Cir. 2019) ("[L]aw enforcement officers may conduct a warrantless search of a cell phone under the border search exception where the officers possess sufficient individualized suspicion of transnational criminal activity"); *United States v. Wanjiku*, 919 F.3d 472, 485 (7th Cir. 2019) ("[N]o circuit court, before or after *Riley*, has required more than reasonable suspicion for a border search of cell phones or

electronically-stored data."); *and Kolsuz*, 890 F.3d at 143 ("Government agents forensically searched Kolsuz's phone because they had reason to believe—and good reason to believe, in the form of two suitcases filled with firearms parts—that Kolsuz was attempting to export firearms illegally and without a license."); *with United States v. Touset*, 890 F.3d 1227, 1234 (11th Cir. 2018) ("Although the Supreme Court stressed in *Riley* that the search of a cell phone risks a significant intrusion on privacy, our decision in *Vergara* made clear that *Riley*, which involved the search-incident-to-arrest exception, does not apply to searches at the border.").

Courts have allowed far more intrusive searches of the person without a warrant or probable cause under the border search doctrine. Strip searches of the person are permissible as part of a border search where there is reasonable suspicion. *United States v. McMurray*, 747 F.2d 1417, 1420 (11th Cir. 1984); *United States v. Rodriguez*, 592 F.2d 553, 556 (9th Cir. 1979); *United States v. Asbury*, 586 F.2d 973, 975-76 (2d Cir. 1978); *United States v. Himmelwright*, 551 F.2d 991, 994-95 (5th Cir. 1977). So too an x-ray of the person, *United States v. Vega-Barvo*, 729 F.2d 1341, 1349 (11th Cir. 1984), or a "search [of] the alimentary canal of a traveler," *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (citing *Montoya de Hernandez*, 473 U.S. at 541). In a similar vein, no court has required more than reasonable suspicion to justify drilling into a vehicle or container, even though it causes permanent damage. *United States v. Rivas*, 157 F.3d 364, 366-67 (5th Cir. 1998); *Robles*, 45 F.3d at 5; *United States v. Carreon*, 872 F.2d 1436, 1440-41 (10th Cir. 1989); *cf. United States v. Chaudhry*, 424 F.3d 1051, 1053 (9th Cir. 2005) (drilling of single hole in pickup truck bed during border search was lawful even in the absence of individualized suspicion). In sum, even the most intrusive searches require no more than reasonable suspicion when conducted at the border.

The defendant argues that *Riley v. California*, 573 U.S. 373 (2014) and, to a lesser extent *Carpenter v. United States*, 138 S. Ct. 2206 (2018), impose a probable cause and warrant requirement for border searches of electronic devices.[6] The defendant is mistaken.

As noted above, even after *Riley*, no court has required more than reasonable suspicion for border searches of electronic devices. *See Alasaad*, 2021 WL 521570; *Aigbekaen*, 943 at 719 n.4; *United States v. Cano*, 934 F.3d 1002, 1015 (9th Cir. 2019); *Kolsuz*, 890 F.3d at 143; *Touset*, 890 F.3d 1227 at 1234. In *Riley* itself, the Supreme Court observed that its holding was limited to the search-incident-to-arrest context, stating that while "the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone." 573 U.S. at 401-02; *see United States v. Gonzales*, 658 F. App'x 867, 870 (9th Cir. 2016) ("*Riley* did not address border searches, and expressly acknowledged" that phone searches may be justified under warrant exceptions other than the search-incident-to-arrest exception); *United States v. Saboonchi*, 48 F. Supp. 3d 815, 819 (D. Md. 2014) ("*Riley* did not diminish the Government's interests in protecting the border or the scope of the border search exception.").

The border search doctrine is markedly different from the search-incident-to-arrest exception to the Fourth Amendment warrant requirement at issue in *Riley*. The search-incident-to-arrest exception allows for a search of the person and the immediate vicinity of the arrestee. That is fully consistent with the limited purposes of the exception, which are to locate any weapons that might endanger the arresting officer and to prevent the destruction of evidence. *See Riley*, 573

[6] Here, SA Depke reviewed a USB drive, a SIM card, and a Micro SD card, which are portable electronic storage devices. *Riley* concerned cellular telephones, which arguably hold more sensitive personal information than these devices. *Carpenter*, which concerned historical cell site information, is inapposite.

U.S. at 383 (quoting *Chimel v. California*, 395 U.S. 752, 762-63 (1969)). As the Supreme Court noted in *Riley*, "there are no comparable risks" of harm to the arresting officer or destruction of evidence "when the search is of digital data." *Id.* at 386.

The border search doctrine, by contrast, serves different and broader purposes, namely protecting the nation's core sovereignty in controlling the entry and exit of persons and property to protect national security and threats to the citizenry. *E.g.*, *Almeida-Sanchez v. United States*, 413 U.S. 266, 291 (1973); *United States v. Oriakhi*, 57 F.3d 1290, 1296-1302 (4th Cir. 1995); *Ickes*, 393 F.3d at 505. Unlike with searches incident to arrest, the purposes underlying the border search doctrine apply in full force to searches of electronic media, which can contain contraband or material (such as classified information, export-controlled items or malware) that, if illicitly transferred beyond our borders, could pose a direct threat to our national security. Notwithstanding the defendant's argument, these concerns apply with equal force to inbound *and outbound* travelers. *See United States v. Odutayo*, 406 F.3d 386, 391–92 (5th Cir. 2005) (holding border search exception applies to outgoing baggage); *United States v. Boumelhem*, 339 F.3d 414, 419–20 (6th Cir. 2003) (establishing that border search exception applies to outgoing cargo container); *United States v. Beras*, 183 F.3d 22, 26 (1st Cir. 1999) (concluding that pat down of outgoing traveler was permitted under the border search exception); *United States v. Udofot*, 711 F.2d 831, 839 (8th Cir. 1983). And the greater storage capacity of electronic devices enables greater harm through the smuggling of, for example, large amounts of classified or proprietary data.

The defendant also argues that the warrantless search of his Devices must be limited to the detection of contraband. The defendant relies on *United States v. Cano*, 934 F.3d 1002, 1017-18 (9th Cir. 2019), *petition for cert. pending*, No. 20-1043 (filed Jan. 29, 2021) (holding that all "cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for

digital contraband" on the device itself—not for "mere evidence" of past, present, or future efforts to transport physical contraband or otherwise violate the laws enforced at the border). Of course, *Cano* is not binding on this Court, and it is an outlier and in conflict with at least three circuits. *See Alasaad*, 2021 WL 521570 at *8 ("We cannot agree with its narrow view of the border search exception because *Cano* fails to appreciate the full range of justifications for the border search exception beyond the prevention of contraband itself entering the country."); *United States v. Williams*, 942 F.3d 1187, 1191 (10th Cir. 2019) (rejecting defendant's argument that customs officers are exclusively tasked with upholding customs laws and rooting out the importation of contraband); *Kolsuz*, 890 F.3d at 143 (upholding border search of defendant's phone even though contraband had been detected in his luggage).[7]

The government's interest in "protecting[] its territorial integrity," *Flores-Montano*, 541 U.S. at 153, undoubtedly encompasses preventing the entry of contraband, digital or physical, and the Court's leading border-search cases happened to involve drug smuggling. But nothing in the language or logic of those decisions suggests that the United States' sovereign prerogative to safeguard its borders is limited to interdicting incoming illicit goods. At a minimum, the doctrine also encompasses, for example, searches aimed at uncovering evidence of other border-related unlawful activity, whether completed or ongoing. *See Alasaad*, 2021 WL 521570 at *8 ("Advanced border searches of electronic devices may be used to search for contraband, evidence of contraband, or for evidence of activity in violation of the laws enforced or administered by CBP or ICE."); *Kolsuz*, 890 F.3d at 144 (finding that a search conducted to uncover information about

[7] In *Aigbekaen*, which is also cited by the defendant, the Fourth Circuit clarified that the border search must have some nexus to transnational criminal activity. 942 F.3d at 719 n.4. That requirement is met here, because the FBI reasonably suspected that the defendant was smuggling stolen trade secret information to foreign competitors.

an ongoing transnational crime fits "within the core rationale" underlying the border search exception). Authority to search for contraband logically must include authority to search for evidence of a planned attempt to import or export contraband.

Even if the Court does apply *Cano*, suppression is not warranted. CBP and the FBI reasonably believed that the defendant possessed stolen trade secrets, which constitute contraband. Because the defendant's possession of the stolen trade secrets was unlawful, CBP and the FBI were authorized to search for them to prevent their export from the United States. *See Kolsuz*, 890 F.3d at 137 ("The fundamental principles of national sovereignty that are the basis for the border search exception, we have explained, apply equally to government efforts to protect and monitor exports from the country as they do to efforts to control imports. Thus, with respect to exit searches, the border search exception is justified by the government's power to regulate the export of currency and other goods" (internal citations and quotations omitted)).

2. SA Depke's Search Was Supported by Reasonable Suspicion

SA Depke conducted a cursory review of the three memory cards. Although the CART team created full forensic images, SA Depke only performed keyword searches. As discussed above, reasonable suspicion is the highest standard applied in the border search context. While the government does not concede that individualized suspicion was required here, see *Touset*, 890 F.3d at 1233, the Court need not reach the question as reasonable suspicion was clearly present.

Reasonable suspicion means a "minimal level of objective justification." *INS v. Delgado*, 466 U.S. 210, 217 (1984); *see Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968) (reasonable suspicion standard is satisfied by "specific and articulable facts" and rational inferences indicating that criminal activity "may be afoot"). The Eighth Circuit has explained that "reasonable suspicion is a 'particularized and objective' basis for suspecting the person who is stopped." *United States v.*

Busto-Torres, 396 F.3d 935, 942 (8th Cir. 2005) (quoting *United States v. Thomas,* 249 F.3d 725, 729 (8th Cir. 2001)). "Whether the particular facts known to the officer amount to an objective and particularized basis for a reasonable suspicion of criminal activity is determined in light of the totality of the circumstances." *Id.* (quoting *United States v. Halls,* 40 F.3d 275, 276 (8th Cir.1994) (citation omitted)). Other courts have explained that reasonable suspicion "is 'considerably less than proof of wrongdoing by a preponderance of the evidence,' and 'obviously less demanding than that for probable cause.'" *United States v. Jones*, 584 F.3d 1083, 1086 (D.C. Cir. 2009) (quoting *United States v. Sokolow*, 490 U.S. 1, 7 (1989)).

Here, prior to reviewing the memory cards, SA Depke knew the defendant (1) had access to information that was proprietary and valuable; (2) communicated with a colleague who was suspected of sharing Monsanto's proprietary information to obtain a job in the PRC; (3) sent information from Monsanto to a competitor in the PRC; (4) emailed corporate-confidential information to his personal email accounts; (5) conducted Google searches about sharing information with third parties and the resulting consequences; (6) had been deceptive and nervous during his exit interview, according to Monsanto employees, particularly when asked about his handling of Monsanto's intellectual property and confronted with the suspicious Google searches; and (7) boarded a one-way flight to the PRC but claimed to be starting a new job in one week at a joint venture in Illinois. Under these circumstances, SA Depke reasonably suspected that the defendant was unlawfully departing the United States with intellectual property he had stolen from Monsanto.

C. The Search of the Devices Was Consistent with the Scope of the Border Search Exception

The defendant also argues that the search of the devices exceeded the scope of the border search exception and violated CBP policy. Both of these arguments miss the mark.

First, the FBI's coordination with CBP does not render the search invalid. By searching the defendant's baggage, detaining the Devices, and providing them to the FBI for review and analysis, CBP was pursuing its own important law enforcement and national security objectives. CBP's duties include enforcing the law at the border, protecting national security, and preventing the import or export of contraband. *See* 6 U.S.C. § 211 (has the responsibility to "ensure the interdiction of persons and goods illegally entering or exiting the United States"; "detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States"; "safeguard the borders of the United States to protect against the entry of dangerous goods"; "enforce and administer all immigration laws"; "deter and prevent the illegal entry of terrorists, terrorist weapons, persons, and contraband"; and "conduct inspections at [] ports of entry to safeguard the United States from terrorism and illegal entry of persons").

The government's interest in "protecting[ ] its territorial integrity," *Flores-Montano*, 541 U.S. at 153, undoubtedly encompasses preventing the entry or exit of contraband, digital or physical. In this case, CBP's coordination with the FBI to detect and prevent economic espionage and the theft of trade secrets soundly serves this purpose.

The Sixth Circuit affirmed a border search of a shipping container under similar circumstances. *See Boumelhem*, 339 F.3d at 428. In that case, the defendant was being investigated by a joint terrorism task force, which was headed by the FBI and had participants from multiple agencies. *Id.* at 417. At the FBI's request, customs agents searched and seized an

outbound shipping container. *Id.* at 417-18. The Sixth Circuit affirmed the district court's denial of suppression, observing that Customs agents "actively cooperated in the search" and had an interest in preventing the export of weapons in violation of federal law. *Id.* at 424.

Boumelhem does have a distinction from this case. There, Customs agents searched the seized shipping container and discovered and logged the evidence. In this case, CBP conducted the initial search and detained the Devices, before transferring them to the FBI for it to render assistance. Nevertheless, these distinctions should not alter the outcome in this case. First, electronic devices are far more portable than a shipping container. Second, CBP sought the FBI's assistance to understand technical information and translate foreign language material. The investigators knew that extensive interpretation, from both Monsanto and a Mandarin-speaker, would be required. FBI St. Louis had previously interacted with Monsanto and was able to share the recovered data with them expeditiously. Likewise, FBI St. Louis had ready access to a Mandarin translator. Therefore, CBP seeking assistance from the FBI was appropriate and consistent with Congress's judgment that customs officers are entitled to "demand the assistance of any person in making any arrest, search, or seizure authorized by any law enforced or administered by customs officers." 19 U.S.C. § 507(a)(2).

Second, CBP and the FBI were not required to review the Devices in Chicago, where they were detained. The Fourth Amendment does not require that detained electronic devices be kept or reviewed at the border. *See, e.g.*, *United States v. Stewart*, 729 F.3d 517, 526 (6th Cir. 2013) (detention of computer at border followed by review at a secondary location twenty miles away was a valid border search); *Cotterman*, 709 F.3d at 962 (detention of computer at border followed by forensic examination at a site 170 miles away was a border search); *United States v. Hassanshahi*, 75 F. Supp. 3d 101 (D.D.C. 2014) (lawful border search where computer was

detained at Los Angeles International Airport and searched in Virginia); *United States v. Saboonchi*, 990 F. Supp. 2d at 548-49, 561 (lawful border search where cell phones were detained at border crossing near Buffalo, shipped, imaged, and returned to defendant in Baltimore; border search can be conducted "over the course of several days, weeks, or months"); *House v. Napolitano*, No. CIV.A. 11–10852–DJC, 2012 WL 1038816 (D. Mass. March 28, 2012) (border search doctrine applied where computer and other devices were seized at Chicago O'Hare International Airport, held for seven weeks, and returned via mail from New York).

Third, the review was not unduly delayed. In total, approximately forty-six days passed from the initial seizure to when the FBI obtained a search warrant to review the Devices. The Supreme Court has not set a bright line for the detention of electronic devices at the border, declining any "hard-and-fast time limits," but directing courts to assess the reasonableness of same in terms of "common sense and ordinary human experience." *Montoya de Hernandez*, 473 U.S. at 543 (internal citation omitted); *see Kolsuz*, 890 F.3d at 136-37 (month-long offsite forensic analysis); *United States v. Thomas-Okeke*, No. CR 2018-0008 2019 WL 2344772 (D.V.I. June 3, 2019) (forensic analysis of cell phone one month after seizure at airport); *United States v. Qin*, No. 18-CR-10205 2020 WL 7024650 (D. Mass. Nov. 30, 2020) (22-day delay in conducting basic search found reasonable because investigators had to obtain passwords from defendant, who was abroad, and find Mandarin speakers to interpret data); *Saboonchi*, 990 F. Supp. 2d (border search can be conducted "over the course of several days, weeks, or months"); *House*, 2012 WL 1038816 at *9 (plaintiff not entitled to summary judgment after 49-day search).

The 46-day period between when CBP detained the Devices and SA Depke obtained a search warrant was reasonable. Approximately four days passed before the Devices arrived in St. Louis. Another six days passed while the FBI imaged the devices, loaded review software on SA

Depke's computer, and trained him to use the software. SA Depke located possibly proprietary information on the SD card and, the very next day, met with Monsanto to discuss the information. Because the information was subject to control measures, SA Depke could only deliver the documents to Monsanto in-person. A Monsanto employee reviewed the information and opined that it likely was trade secret information. Nevertheless, because of the technical nature of the information and the breadth of Monsanto's business, the Monsanto employee needed to confer with subject matter experts. He did not confirm the exact status of the information until June 28, 2017. Once the Monsanto employee told SA Depke that the cards contained stolen trade secret information, the FBI had probable cause to seize the devices.

Approximately 28 days later, SA Depke obtained the search warrant. During this time, SA Depke worked on the affidavit and conferred with the U.S. Attorney's Office and the Department of Justice to ensure that the affidavit was accurate and comprehensive. Under the flexible, "common sense" and "ordinary human experience" test required by the Supreme Court, this period of time was reasonable.

III. Conclusion

For the foregoing reasons, the government respectfully requests that this Court deny the defendant's motion to suppress.

Respectfully submitted,

SAYLER A. FLEMING
United States Attorney

By: /s/*Matthew T. Drake*
MATTHEW T. DRAKE, #46499MO

/s/Gwendolyn E. Carroll
GWENDOLYN E. CARROLL, #4657003NY
Assistant United States Attorneys
111 South Tenth Street, 20th Floor
Saint Louis, Missouri 63102
(314) 539-2200

/s/ Adam L. Small
Adam L. Small
Trial Attorney
Counterintelligence and Export Control Section
National Security Division
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
Tel: (202) 616-2431
Email: Adam.Small@usdoj.gov

Jeff Pearlman (DC: 466-901)
Senior Counsel
Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice
1301 New York Avenue, Suite 600
Washington, DC 20005
(202) 579-6543
(202) 514-6113 (facsimile)
Jeffrey.Pearlman2@usdoj.gov

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on March 5, 2021, the foregoing was filed electronically with the Clerk of the Court to be served by operation of the Court's electronic filing system upon all parties and counsel of record.

/s/ Adam L. Small
Adam L. Small

s/Matthew T. Drake
MATTHEW T. DRAKE, #46499MO

s/Gwendolyn E. Carroll
GWENDOLYN E. CARROLL, #4657003NY